

**XIII
JORNADAS
STIC
CCN-CERT**



**Visión práctica del
Catálogo de
Productos del CCN**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Miguel Viedma Astudillo

Clover Technologies S.L.

miguel.viedma@cloverttechnologies.es

Fidel Paniagua Diez

Clover Technologies S.L.

fidel.panigua@cloverttechnologies.es

Índice

- 1. Nuestra empresa**
- 2. Catálogo de Productos STIC, CPSTIC**
- 3. Proceso de inclusión en el CPSTIC**
- 4. Uso del CPSTIC**

Laboratorio de Evaluación

Laboratorio de Evaluación del ENECSTI acreditado para realizar ejecuciones de acuerdo a las metodologías **Common Criteria** y **LINCE**.

Organismo de Certificación | Centro Criptológico Nacional

OC-CN

SOBRE OC PRODUCTOS CERTIFICADOS CATÁLOGO PRODUCTOS STIC TIPOS DE CERTIFICACIÓN SOLICITUDES Y FORMULARIOS

Clover Technologies

Responsable: Fidel Paniagua

Avenida Juan Caramuel nº 1
28918. Leganés (Madrid)
Teléfono: 918371005

Common Criteria
EAL1

LINCE

<http://www.doverttechnologies.es/>
evaluaciones@cloverttechnologies.es

<https://oc.ccn.cni.es/index.php/es/acreditacion-de-laboratorios/laboratorios-acreditados>

CCN
centro criptológico nacional

CERTIFICATE
CCN-AT-2/2019

Authorization as ENECSTI ITSEF for "CLOVER TECHNOLOGIES"

Pursuant to the authority vested in me under Act 11/2002 regulating the National Intelligence Centre, and under Article 1 and Article 2.2.c of Royal Decree 421/2004 of March 12th regulating the National Cryptologic Centre, I hereby:

Approve "CLOVER TECHNOLOGIES", registered at "Avenida de la Aurora 55, 4ºC, 29006, Malaga" as Information Technology Security Evaluation Facility (ITSEF) within the National IT Security Evaluation and Certification Scheme (ENECSTI), to perform IT security evaluations according to "Common Criteria for Information Technology Security Evaluation" and "Common Methodology for Information Technology Security Evaluation" up to level EAL1, handling unclassified information and products.

Madrid, 25th February 2019
Secretary of State Director

Félix Sanz Roldán

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

Nuestra empresa



CONSULTORÍA

Acreditación de sistemas TIC.
Análisis y evaluación de riesgos en sistemas e infraestructuras
Análisis de seguridad de dispositivos y sistemas
Cursos de formación y concienciación en ciberseguridad.

EVALUACIÓN

Evaluación de productos de seguridad TIC: Common Criteria y LINCE.

Redacción de guías de instalación, configuración y uso seguro de sistemas.

OPERACIÓN

Configuración segura de sistemas y herramientas de ciberseguridad.

Análisis y estudio de **malware**.

Soporte en respuesta a **incidentes** de seguridad

DESARROLLO

Sistemas de **control de acceso**.

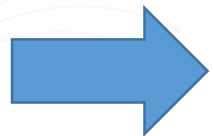
Sistemas basados en **blockchain**.

Sistemas **web** y bases de datos.

Catálogo de Productos STIC

Definición

- El catálogo ofrece un listado de productos de Seguridad TIC, con unas garantías de seguridad contrastadas, a organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren afectados por el Esquema Nacional de Seguridad (ENS) o manejen información clasificada.



Tipo de Producto	Información manejada
APROBADO	Información Clasificada
CUALIFICADO	Información Sensible – ENS



Catálogo de Productos STIC

Esquema Nacional de Seguridad

- **Artículo 18**

*“En la **adquisición de productos de seguridad** de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan **certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición**, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.”*

- **Medidas Anexo 2: “Componentes certificados [op.pl.5]” - Categoría ALTA**

*Se utilizarán **sistemas, productos o equipos** cuyas funcionalidades de seguridad y su nivel hayan sido **evaluados conforme a normas europeas o internacionales** y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.*

Catálogo de Productos STIC

Definición

- El CCN ha definido una **taxonomía** de productos de seguridad TIC, organizados en diferentes **categorías** que se dividen, a su vez, en **familias**.
- Cada producto incluido en el apartado de **Productos Cualificados del CPSTIC** debe cumplir con los **Requisitos Fundamentales de Seguridad (RFS)** definidos para cada familia en forma de anexo de la guía CCN-STIC 140.



Guía de Seguridad de las TIC
CCN-STIC 105

Catálogo de Productos de Seguridad de las Tecnologías de la
Información y la Comunicación



Octubre de 2019



Catálogo de Productos STIC

Documentación de referencia

Referencia	Documento
CCN-STIC-105	Catálogo de Productos de Seguridad TIC (CPSTIC)
CCN-STIC-106	Procedimiento de inclusión de productos de seguridad TIC en el CPSTIC
CCN-STIC-140	Taxonomía de referencia para productos de seguridad TIC
PO-09	Procedimiento de cualificación de productos STIC en el ENECSTI

Catálogo de Productos STIC

Categorías y Familias

Control de acceso

- NAC
- Dispositivos Single Sign-on
- Dispositivos biométricos
- Dispositivos autenticación
- PAM

Explotación de la seguridad

- Antivirus/EPP
- EDR
- Filtrado de navegación
- MDM
- SIEM
- Dispositivos gestión claves criptográficas

Monitorización de la seguridad

- Dispositivos de prevención de intrusiones
- Honeypot / HoneyNet
- Captura, monitorización y análisis de tráfico.

Protección de las Comunicaciones

- Enrutadores
- Switches
- Proxies
- Cortafuegos
- VPN
- Dispositivos de red inalámbricos

Protección de la información y soportes de información

- Cifrado de datos
- Cifrado offline
- DLP
- Firma Electrónica
- Borrado Seguro

Protección de equipos y servicios

- Dispositivos móviles
- Copias de seguridad
- Sistemas operativos
- Virtualización
- Plataformas confiables
- Tarjetas inteligentes

Catálogo de Productos STIC

Ejemplo: Familia Enrutadores – Requisitos ENS Alto



Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC -
Anexo D.1: Enrutadores



Noviembre 2017

- **REQ 1:** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma Common Criteria:
 - *CCDB - Collaborative Protection Profile for Network Devices v1.0*
 - *NIAP - Protection Profile for Network Devices v1.1*
- **REQ 2:** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la **DS** deberá contener al menos los **RFS** del perfil **CPP_ND_v1.0** con un nivel de confianza **EAL2** o superior.
- **REQ 3:** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse en la guía **CCN-STIC-807** Criptología de empleo en el ENS (Categoría ALTA).

<https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3923-guia-140-anexo-d-1-enrutadores/file.html>

Catálogo de Productos STIC

Ejemplo: Familia Enrutadores – Requisitos ENS Alto

collaborative Protection Profile for Network Devices

collaborative Protection Profile for
Network Devices

Version 2.0
5-May-2017

- Amenazas
- Asunciones
- Objetivos
- Requisitos Funcionales de seguridad

6.4.2.1 FCS_COP.1 Cryptographic Operation

FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
--------------------------	--

FCS_COP.1.1/DataEncryption The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm [*assignment: AES used in [selection: CBC, CTR, GCM] mode and cryptographic key sizes [assignment: 128 bits, 192 bits, 256 bits] that meet the following: [assignment: AES as specified in ISO 18033-3, [selection: CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].*

https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V2.0.pdf

Fases



Proceso de inclusión en el CPSTIC

Solicitud

1. Envío de la solicitud (**FOR 006**) de inclusión de producto en el catálogo por parte del fabricante, suministrador o organismo de la Administración. Está se compone de:
 1. Datos del solicitante.
 2. Persona de contacto.
 3. Organismo proponente (aval formal).
 4. Información del producto.
 5. Certificación Common Criteria o LINCE.
 6. Taxonomía del producto.
 7. Declaración de aceptar y conocer los requisitos de inclusión de productos de seguridad TIC cualificados. (FOR 007)
 8. Adjuntos (ficheros a adjuntar).



¿Qué categoría y familia me aplica?



¿Puede mi producto estar en más de una categoría o familia?



¿Puede mi producto ofrecer funcionalidades de seguridad extra a las especificadas en los RFS de la familia?



Si mi producto soporta opciones no seguras, ¿para poder estar en el catálogo es necesario eliminarlas del producto?

Proceso de inclusión en el CPSTIC

Solicitud - Adjuntos

1. Declaración de Seguridad - **DS**
2. **Informe preliminar de Conformidad** de los RFS
 1. Todas los RFS están incluidos en la DS
 2. RFS implementados por el producto pero no incluidos en la DS
 3. RFS no implementados por el producto
3. Listado de **algoritmos criptográficos** empleados en el producto (*)
4. Propuesta de procedimiento de empleo seguro **PE** del producto (*)

(*) *Entrega opcional en la fase de solicitud*

Proceso de inclusión en el CPSTIC

Análisis

1. Estudio del grado de cumplimiento con los RFS
2. Estudio de riesgos adicionales no cubierto por los RFS
3. Como resultado, **Informe Técnico de Cualificación**:
 1. Grado de cumplimiento de los RFS en base a certificaciones previas
 2. Riesgos no cubiertos por la certificación
 3. Evaluaciones y pruebas complementarias requeridas

Proceso de inclusión en el CPSTIC

Análisis – Grado de cumplimiento con los RFS – ENS Alto

Evaluaciones requeridas para cualificación ENS ALTO		
Certificaciones previas	Evaluaciones requeridas	
	Evaluaciones adicionales	Evaluaciones criptográficas
Certificación <i>Common Criteria</i> con TODOS RFS	Depende del Análisis de Riesgos	Validación algoritmos CCN-STIC-807 Criptología de empleo en el ENS (Categoría Alta)
Certificación <i>Common Criteria</i> no incluye TODOS RFS	Recertificación <i>Common Criteria</i> o Evaluación STIC	
Sin Certificación <i>Common Criteria</i>	Certificación <i>Common Criteria</i> con todos RFS	



Proceso de inclusión en el CPSTIC

Análisis – Grado de cumplimiento con los RFS – ENS MEDIA y BÁSICA

Evaluaciones requeridas para cualificación ENS ALTO		
Certificaciones previas	Evaluaciones requeridas	
	Evaluaciones adicionales	Evaluaciones criptográficas
Certificación <i>Common Criteria</i> LINCE con TODOS RFS	Depende del Análisis de Riesgos	Validación algoritmos CCN-STIC-807 Criptología de empleo en el ENS (Categoría Media y Básica)
Certificación <i>Common Criteria</i> no incluye TODOS RFS	Evaluación STIC	
Sin Certificación	Certificación LINCE con todos RFS	



Proceso de inclusión en el CPSTIC

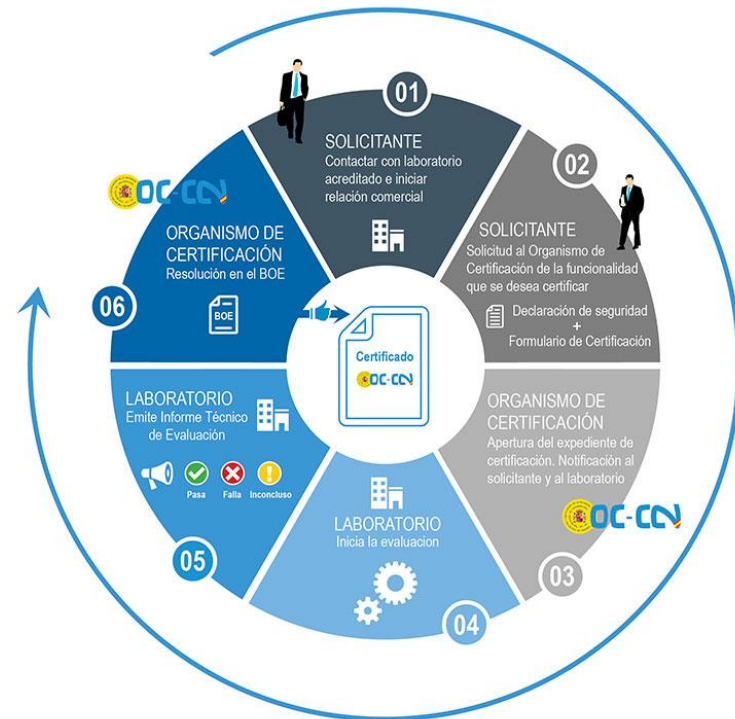
Evaluación

1. Se cumple con todos los RFS y no hay riesgos adicionales.
 1. CCN realiza una revisión básica del producto.
2. El producto no tiene riesgos adicionales pero no cumple con los RFS.
 1. El producto debe estar considerado de interés estratégico para la Administración (avalado formalmente).
 2. No existe en el CPSTIC un producto cualificado con la misma funcionalidad.
 3. Un laboratorio acreditado verifica el cumplimiento del producto con la CCN-STIC-807.
3. El producto no cumple todos los RFS ni cumple los requisitos de excepcionalidad:
 1. Una laboratorio acreditado realizará una evaluación del producto basada en los RFS que debe cumplir.

Todos los productos que cumplan con alguno de estos tres casos, el CCN propondrá la inclusión del producto en el CPSTIC como producto **Cualificado**.

Proceso de inclusión en el CPSTIC

Evaluación - Certificación



Proceso de Certificación: entre 3 y 18 meses

Criterios y metodologías de Evaluación



<https://oc.ccn.cni.es/index.php/es/tipos-de-certificacion/certificacion-funcional/criterios-y-metodologias>

Proceso de inclusión en el CPSTIC

Certificado

Certificado de “**Producto Cualificado de Seguridad TIC**” que será firmado por el **Secretario de Estado Director del Centro Nacional de Inteligencia**, que como Director del Centro Criptológico Nacional es la Autoridad de Certificación de la Seguridad de las Tecnologías de la Información.

(RD 21/2004 de 12 de Marzo, Art.1).

CERTIFICADO DE CUALIFICACIÓN	
<<Referencia expediente de cualificación>>	
<<Declaración de seguridad>>	
Versión:	<<version>>
Fabricante:	<<fabricante>>
Familia:	<<familias del CPSTIC en las que se incluye>>
Categoría ENS:	Alta
Válido hasta:	<<dd>>/<<mm>>/<<aaaa>>
De acuerdo con las facultades que me confiere la Ley 11/2002 de 6 de mayo, reguladora del CNI, y al amparo de lo dispuesto en los artículos 1 y 2.2.c, del RD 421/2004 de 12 de marzo, por el que se regula el Centro Criptológico Nacional, y el artículo 18 del RD 3/2010, de 8 de enero, modificado por el RD 951/2015, de 23 de octubre: Certifico que el producto arriba referido, con las restricciones indicadas en el procedimiento de empleo CCN-STIC-<<nnnn>> <<nombre guía>>, cumple con los requisitos establecidos en las guías CCN-STIC-106 y en la CCN-STIC-140 para la familia de productos arriba indicada y por lo tanto se considera Producto Cualificado para la categoría ENS Alta.	
	Madrid, <<dd>>/<<mm>>/<<aaaa>> El Secretario de Estado <<Nombre del Secretario de Estado>>
	

Proceso de inclusión en el CPSTIC

Mantenimiento - Actualizaciones

1. Ante una actualización el fabricante debe entregar al CCN un **informe de cambios** y del impacto de dichos cambios en la seguridad del producto.
2. El CCN revisa los cambios de esta nueva versión.
3. Si el producto sigue garantizando las características de seguridad evaluadas, se expide una adenda al certificado de Producto Cualificado de Seguridad TIC para dicha versión.
4. Si no es así, se podría requerir comenzar el proceso de cualificación de la nueva versión del producto.

Proceso de inclusión en el CPSTIC

Mantenimiento - Exclusión

1. **Caducidad del certificado** de Producto Cualificado de Seguridad TIC.
2. **Revocación** de alguna de las **certificaciones** requeridas al producto.
3. Que no cumpla con los **RFS vigentes** en el momento de la revisión de validez.
4. El producto presenta **vulnerabilidades críticas** no corregidas.

Uso del CPSTIC

Consumidor Final del CPSTIC



¿Un producto **Cualificado** es lo mismo que uno **Certificado** Common Criteria?

- Common Criteria aporta una metodología de evaluación, responde al **¿cómo?** pero no dice nada del **¿qué?**, por ello, cabría preguntarse: **¿qué funcionalidades de seguridad incluyo en mi certificación?**
- La funcionalidad de seguridad, **RFS**, definidas en la **Declaración de Seguridad** la determina el **Fabricante**.



Uso del CPSTIC

Consumidor Final del CPSTIC



¿Es **obligatorio** el uso del CPSTIC para la **adquisición de productos para el ENS**?

- **NO** es obligatorio, aunque **sí** conveniente.
- Cuando el sistema en que se vaya a utilizar el producto esté afectado por el ENS deberá cumplir con la normativa que lo regula, en la que se establece de manera específica la obligatoriedad de utilizar productos que tengan **certificadas las funcionalidades de seguridad** relacionadas con el objeto de su adquisición cuando el sistema esté clasificado como **Categoría ALTA**, y la conveniencia, con carácter general, de utilizarlos para el resto de sistemas.
- Cualquier responsable de la adquisición de productos TIC, puede **comprobar** si un producto reúne las garantías de seguridad requeridas.

Uso del CPSTIC

Consulta

Versión PDF



Guía de Seguridad de las TIC
CCN-STIC 105

Catálogo de Productos de Seguridad de las Tecnologías de la
Información y la Comunicación



Octubre de 2019

Versión Web

Organismo de Certificación | Centro Criptológico Nacional

OC-CCN

SOBRE OC PRODUCTOS CERTIFICADOS CATÁLOGO PRODUCTOS STIC TIPOS DE CERTIFICACIÓN SOLIC

INICIO » CATÁLOGO PRODUCTOS STIC » LISTADO DE PRODUCTOS CUALIFICADOS

PRODUCTOS STIC CUALIFICADOS

Filtros:

Buscar:

Nombre	Categoría	Fabricante	Familia
ADSS Server SAM Appliance 6.0	Protección de la Información y los Soportes de información	ASCERTIA	Herramientas para fii electrónica
X930 Series AlliedWare Plus. Software Version 5.4.6-1	Protección de las Comunicaciones	Allied Telesys	Switches
Galaxy Note 9 (SM-N960) Android 8	Protección de equipos y servicios	Samsung Electronics Co., Ltd	Dispositivos móviles
Galaxy Tab S4 (SM-T830 / SM-T835) Android 8	Protección de equipos y servicios	Samsung Electronics Co., Ltd	Dispositivos móviles

<https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html>

<https://oc.ccn.cni.es/index.php/es/catalogo-productos-stic/listado-productos-cualificados>

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional